CA Nimsoft Monitor Server

Notas da Versão e Guia de Atualização

7.6



Histórico de revisões do documento

Versão do NMS	Data	Alterações
7.60	Junho de 2014	Revisado para NMS 7.60
7.50	Maio de 2014	Problemas conhecidos revisados
7.50	Março de 2014	Revisado para NMS 7.50
7.10	Dezembro de 2013	Revisado para NMS 7.10
7.00	Setembro de 2013	Revisado para NMS 7.00
6.50	Março de 2013	Revisado para NMS 6.50
6.20	Dezembro de 2012	Revisado para NMS 6.20
6.10	Setembro de 2012	Atualizado e revisado para NMS 6.10
6.00	Junho de 2012	Revisado para 6.00
5.61	Abril de 2012	Observação sobre scripts de atualização grandes do banco de dados MySQL
5.61	Março de 2012	Atualizações na documentação
5.61	Fevereiro de 2012	Correções e atualizações na documentação
5.61	Janeiro de 2012	Revisado para NMS versão 5.61
5.60	Dezembro de 2011	Revisado para NSM 5.60

Aviso de copyright do CA Nimsoft Monitor

As informações legais sobre software de domínio público e de terceiros usado na solução do Nimsoft Monitor estão documentadas em *Licenças de Terceiros e Termos de Uso do Nimsoft Monitor (*http://docs.nimsoft.com/prodhelp/en_US/Library/Legal.html*).*

Entrar em contato com a CA

Entrar em contato com a CA Support

Para sua conveniência, a CA Technologies oferece um site onde é possível acessar as informações necessárias a seus produtos da CA Technologies para escritório doméstico, pequena empresa e corporativos. Em http://ca.com/support, é possível acessar os seguintes recursos:

- Informações para contato online e telefônico, assistência técnica e atendimento ao cliente
- Informações sobre fóruns e comunidades de usuário
- Downloads de produto e documentação
- Políticas e diretrizes de CA Support
- Outros recursos úteis adequados ao seu produto

Fornecendo comentários sobre a documentação do produto

Enviar comentários ou perguntas sobre a documentação de produtos da Nimsoft da CA Technologies para nimsoft.techpubs @ ca.com.

Se desejar fornecer comentários sobre a documentação geral dos produtos da CA Technologies, responda nossa breve pesquisa do cliente, disponível no site de CA Support, encontrado em http://ca.com/docs.

Índice

Capítulo 1: Funcionalidades novas e alteradas

O NMS (Nimsoft Monitor Server) 7.60 é uma release principal que melhora a estabilidade, a escalabilidade, o desempenho, os recursos e a funcionalidade do produto, adicionando estes novos recursos importantes:

Hub e robô

- Novos programas de instalação de robô nativos e suporte ADE a:
  - AIX
  - zLinux
- Robô 7.60 para zLinux.
- A porta do primeiro probe do robô tem como padrão 48000.
- Nova documentação:
  - Adição ou remoção de um robô passivo
  - Gerenciamento do movimento de robô

Detecção

- Caracterização de dispositivos SNMP expandida para informações sobre o sistema operacional AIX, dispositivos Cisco Unified Communications e dispositivos HP Tipping Point.
- Adicionado o parâmetro de configuração excluded_ip_addresses à correlação de endereço IP. O valor do parâmetro oferece suporte a uma lista separada por vírgulas de qualquer combinação de endereços IP individuais, intervalos de endereços IP e sub-redes IP em notação CIDR (por exemplo, 1.2.3.4, 10.1.2.3-99, 172.1.2/24).
- Adicionados os parâmetros de configuração excluded_fqdns e excluded_domains à correlação de FQDN (Fully Qualified Domain Name – Nome de Domínio Totalmente Qualificado).
- Cm_data_import pode importar perfis de autenticação SNMP V1, V2c e V3.

Capítulo 2: Requisitos

Sistemas com suporte

Para obter mais informações sobre:

- Requisitos de sistema do NMS, consulte o Guia de Instalação do NMS.
- Sistemas operacionais, bancos de dados, navegadores e versões JRE com suporte, consulte a Matriz de suporte de compatibilidade da Nimsoft.
- Para componentes que estão sendo substituídos ou que não têm mais suporte, consulte os Anúncios de suporte e encerramento de vendas do Nimsoft.
- **Observação:** o NMS 6.5 ou posterior requer a versão de 64 bits de um sistema operacional suportado. Se estiver migrando de um sistema de 32 bits, entre em contato com o Suporte da Nimsoft http://support.nimsoft.com para obter assistência.

Componente Infraestrutura do Nimsoft

A Infraestrutura do Nimsoft faz parte da instalação do servidor do Nimsoft. Se desejar instalar apenas a Infraestrutura do Nimsoft (hubs, robôs ou probes) em um sistema UNIX® adicional, os sistemas UNIX® a seguir têm suporte:

- AIX
- HP-UX
- Linux
- Solaris

Mais informações também estão disponíveis online, na Matriz de suporte de compatibilidade da Nimsoft, que é atualizada regularmente.

Requisitos do sistema adicionais

- O mecanismo de dados requer:
  - libstdc++.so.5 (libstdc++-3.3.4-11.x86_64.rpm) em distribuições do Linux OpensUsE
  - Windows 2008 R2 SP1 em distribuições do Windows
- O banco de dados não deve diferenciar maiúsculas de minúsculas ao controlar as consultas.
- A verificação de espaço livre do banco de dados não está implementada para Oracle e MySQL.
- Se desejaR que a detecção localize sistemas IPv4 e IPv6, discovery_agent precisará ser executado no sistema IPv4/IPv6 de pilha dual.

Idiomas com suporte

O Nimsoft Monitor está disponível em inglês, alemão, espanhol, português do Brasil, chinês simplificado, japonês e coreano.

Capítulo 3: Considerações

Esta seção descreve as características encontradas nesta release que afetam a versão 7.6 da instalação, da atualização, da localização ou do comportamento em geral do NMS.

Tópicos:

Dimensionamento do sistema

Para obter as mais recentes informações de dimensionamento, consulte Preparação dos servidores no *Guia de Instalação do NMS*.

Privilégios de logon necessários

Use um logon com privilégios de *administrador* ou *raiz* ao instalar ou atualizar para o NMS 7.6.

Instalar dois ou mais hubs

É recomendável que instale pelo menos dois hubs no mesmo domínio e rede, de modo que, se o servidor que hospeda o hub principal falhar, você não perca dados de segurança e do usuário (definições de usuário do Nimsoft, ACLS, etc.). Com mais de um hub, essas informações são espelhadas entre os hubs.

Sincronização do relógio e programações de manutenção

Para garantir que as programações de manutenção iniciem e parem nas horas desejadas, os relógios do sistema nos servidores a seguir devem estar sincronizados:

- Servidor do NMS (hub principal, incluído o probe maintenance_mode)
- Servidor do banco de dados do NIS
- Servidor(es) do NAS
- Servidor(es) do UMP

Relógios fora de sincronia podem resultar em alarmes incorretos ou ausentes. Por exemplo, suponha que o relógio no servidor do UMP esteja 30 minutos adiantado em relação ao servidor do NAS. Você coloca o seu servidor web em uma programação de manutenção que vai de 9:00 às 11:00.

- Às 9:00, você coloca o servidor web offline para manutenção. Como a hora do servidor do NAS é 8:30, ele não suprime os alarmes na hora prevista.
- Às 11:00, você colocar o servidor web novamente online. No entanto, como a hora do servidor do NAS é 10:30, ele irá suprimir os alarmes por mais 30 minutos.

Para obter informações sobre como usar o NTP (Network Time Protocol - Protocolo de Tempo de Rede) para sincronizar os servidores, vá para o site de distribuição de NTP em http://doc.ntp.org http://doc.ntp.org.

Desative o qos_processor antes de instalar o UMP

Ao instalar ou atualizar o UMP com o MySQL, desative o probe qos_processor antes de executar o programa de instalação do UMP. Quando o UMP estiver instalado, o processador de QoS poderá ser reativado.

Atualizar o probe Gerenciador de provisionamento (ppm)

Para certificar-se de que tem acesso à funcionalidade do Console de administração mais recente, recomendamos que faça download da versão mais recente do probe PPM (Probe Provisioning Manager – Gerenciador de Provisionamento de Probe) para todos os hubs no domínio *após* a atualização do NMS. Use o Console de administração ou o Gerenciador de infraestrutura para implantar o probe PPM no arquivo do probe no site de suporte do CA Nimsoft (support.nimsoft.com).

Taxa de inserção do processador de QoS e tamanho de heap do Java

Na operação normal, a taxa de inserção máxima em um sistema no qual qos_processor e data_engine é executado ao mesmo tempo é 15.000 inserções por segundo. A taxa de inserção máxima real pode variar de acordo com o desempenho do hardware usado para a instalação do NMS. Essa taxa é amplamente independente do tipo de banco de dados.

O volume de memória do probe qos_processor está diretamente correlacionado com o tamanho da tabela S_QOS_DATA no banco de dados. Defina o tamanho máximo de heap do Java de forma adequada:

Número de objetos de QoS	Tamanho máximo da heap do Java
Menos de 300.000	1 GB (padrão)
300.000 – 1.000.000	1,5 GB
Mais que 1.000.000	2,5 GB

Capítulo 4: Atualizando o servidor do Nimsoft

Esta seção explica como atualizar para o NMS 7.6.

Esse processo consiste em uma cadeia de atualizações para os módulos instalados no momento. **NÃO** reinicie o sistema até que todos os módulos tenham sido instalados, até mesmo se receber solicitações do sistema para reiniciar em pontos intermediários do processo.

Antes de atualizar

Os programas de instalação do NMS (GUI, console e silencioso) permitem atualizar o NMS facilmente. Ao atualizar, sua configuração (nomes de domínio e hub, endereços IP, contas de usuário, senhas, etc.) é mantida.

Antes de executar o programa de instalação:

- **Instale o Windows 2008 R2 SP1**

  Em sistemas Windows 2008 R2, instale o Service Pack 1 antes de atualizar o NMS.

- **Desative o encaminhamento de pacotes e limpe a fila de tarefas do distsrv.**

  O encaminhamento de pacotes está configurado na GUI do probe distsrv. Para exibir a fila, selecione Tools > Distribution no Infrastructure Manager. A atualização falhará se a fila de tarefas do distsrv tiver tarefas pendentes. Após uma atualização bem-sucedida, reative o encaminhamento de pacotes no distsrv, se desejar.

- **Desativar a manutenção da tabela e do índice no mecanismo de dados**

  Em tabelas muito grandes (mais de 10 GB), a execução da manutenção da tabela será mais demorada do que o esperado se a manutenção da tabela e do índice estiver ativada. Configurar o probe data_engine no Gerenciador de infraestrutura ou Console de administração para desativar esse recurso.

- **Desativar e limpar a lixeira do Oracle**

  Em implantações que possuam um banco de dados do Oracle, a lixeira deve ser desativada antes de fazer a atualização do NMS.

  Importante: se estiver atualizando do NMS 7.5, também será NECESSÁRIO limpar a lixeira ou a atualização falhará.

  a. Use uma ferramenta como o SQL Developer para se conectar ao banco de dados do Oracle.

  b. Limpe a lixeira. Execute:
  ```
  PURGE DBA_RECYCLEBIN
  ```

  c. Desative a lixeira. Execute:
  ```
  ALTER SYSTEM SET recyclebin = OFF DEFERRED;
  ALTER SESSION SET recyclebin = off;
  ```

  d. Verifique se a lixeira está desativada. Execute:
  ```
  show parameter recyclebin;
  ```

- **Remova os probes personalizados do arquivo morto de probes (recomendado).**

  Mova ou exclua os probes personalizados do arquivo morto de probes; mantenha os probes básicos de infraestrutura. Após a conclusão de todas as instalações e atualizações (principalmente para UMP e Unified Reporter), você pode mover os probes seletivamente de volta para o arquivo morto.

- **Faça backup da configuração do hub principal (recomendado)**

Salvar uma cópia do arquivo hub.cfg na pasta Nimsoft\hub. Os parâmetros ideais de tempo limite para o hub atualizado são definidos durante a atualização, substituindo configurações de tempo limite existentes. A Nimsoft recomenda executar o hub atualizado com estes valores ideais para obter um desempenho aprimorado. No entanto, se você deseja reverter para as configurações antigas de tempo limite por qualquer motivo, mantenha um backup do antigo arquivo de configuração do hub.

Atualizando o sistema do NMS

Atualização do modo da GUI

Quando você atualiza o sistema do NMS, a configuração existente é mantida, tornando uma atualização muito mais simples do que uma nova instalação.

Importante: todos os campos das caixas de diálogo do programa de instalação diferenciam maiúsculas de minúsculas.

1. Desative os programas antivírus em execução no servidor (esses programas podem diminuir a velocidade de instalação de forma significativa).

   Observação: ative os programas antivírus imediatamente após a instalação.

2. Verifique se você desativou o encaminhamento de pacotes, limpou a fila de tarefas do distsrv (necessário) e removeu os probes personalizados do arquivo morto de probes (recomendado).
3. Efetue logon no site de Atendimento ao cliente da Nimsoft http://support.nimsoft.com.
4. Faça download e execute o pacote de instalação mais recente do NMS para Windows.
5. Siga os prompts para concluir a instalação. Sempre que possível, o programa de instalação exibe os valores de configuração atuais para sua confirmação.
6. Quando a atualização estiver concluída, certifique-se de:
   - Ativar os programas antivírus novamente, se necessário.
   - Ativar o encaminhamento de pacotes.
   - Mover os probes personalizados de volta para o arquivo morto de probes, se necessário.
   - Atualizar outros componentes (hubs, robôs, consoles de gerenciamento, etc.) na sua implantação do Nimsoft

Atualização do modo de console (somente Linux e Solaris)

Quando você atualiza o sistema do NMS, a configuração existente é mantida, tornando uma atualização muito mais simples do que uma nova instalação.

Siga estas etapas:

1. Desative os programas antivírus em execução no servidor (esses programas podem diminuir a velocidade de instalação de forma significativa).

   Observação: ative os programas antivírus imediatamente após a instalação.

2. Verifique se você desativou o encaminhamento de pacotes, limpou a fila de tarefas do distsrv (necessário) e removeu os probes personalizados do arquivo morto de probes (recomendado).
3. Efetue logon no site de Atendimento ao cliente da Nimsoft http://support.nimsoft.com.
4. Faça download e execute o pacote de instalação mais recente do NMS para Linux ou Solaris (o pacote tem mais de 1 GB, portanto, essa operação pode levar vários minutos).
5. Execute **chmod 755** no arquivo de instalação para torná-lo executável.
6. Execute o programa de instalação. Em uma linha de comando, execute:
   - Linux: **installNMS_linux.bin -i console**
   - Solaris: **installNMS_solaris.bin -i console**
7. Siga os prompts para concluir a instalação. Sempre que possível, o programa de instalação exibe os valores de configuração atuais para sua confirmação.
8. Quando a atualização estiver concluída, certifique-se de:
   - Ativar os programas antivírus novamente, se necessário.
   - Ativar o encaminhamento de pacotes.
   - Mover os probes personalizados de volta para o arquivo morto de probes, se necessário.
   - Atualizar outros componentes (hubs, robôs, consoles de gerenciamento, etc.) na sua implantação do Nimsoft

Atualizando o NMS no Windows, Linux ou Solaris — Modo silencioso

Quando você atualiza o sistema do NMS, a configuração existente é mantida, tornando uma atualização muito mais simples do que uma nova instalação.

Siga estas etapas:

1. Desative os programas antivírus em execução no servidor (esses programas podem diminuir a velocidade de instalação de forma significativa).

   Observação: ative os programas antivírus imediatamente após a instalação.

2. Verifique se você desativou o encaminhamento de pacotes, limpou a fila de tarefas do distsrv (necessário) e removeu os probes personalizados do arquivo morto de probes (recomendado).

3. Efetue logon no site de Atendimento ao cliente da Nimsoft http://support.nimsoft.com.

4. Faça download:

   - Do pacote de instalação mais recente do NMS para seu sistema operacional e arquitetura.
   - Pacote de instalação silenciosa (arquivo .zip)

5. No Linux ou Solaris, execute **chmod 755** no arquivo de instalação para torná-lo executável.

6. Prepare seu arquivo de resposta:

   a. Extraia os modelos de instalação silenciosa.

   b. Localize o arquivo **installer.upgrade.properties** e salve-o como **installer.properties** no mesmo diretório que o programa de instalação.

   c. Adicione sua senha de administrador do NMS à linha **NMS_PASSWORD=** de **installer.properties**.

   d. Salve o arquivo, garantindo que o tipo de arquivo ainda é **PROPERTIES**. Se o tipo de arquivo for **Text Document**, remova a extensão **.txt** (que pode não ser exibida na pasta).

7. Execute o programa de instalação. Em uma linha de comando, execute:
   - Windows: **installNMS.exe -i silent**
   - Linux: **installNMS_linux.bin -i silent**
   - Solaris: **installNMS_solaris.bin -i silent**
8. O programa de instalação descompacta os arquivos e conclui a instalação. Esse processo pode levar vários minutos ou mais. Para ver o andamento da instalação, execute:

```
tail -f /tmp/ia/iaoutput.txt
```

9. O NMS é iniciado. Se por algum motivo não for iniciado, execute:
   - Windows: **net start Nimsoft Robot Watcher**
   - Linux ou Solaris: **cd /etc/init.**d, em seguida, **nimbus start (**ou **/etc/init.d/nimbus start**)
10. Quando a atualização estiver concluída, certifique-se de:
    - Ativar os programas antivírus novamente, se necessário.
    - Ativar o encaminhamento de pacotes.
    - Mover os probes personalizados de volta para o arquivo morto de probes, se necessário.
    - Atualizar os componentes (hubs, robôs, consoles de gerenciamento, etc.) na implantação do Nimsoft.

Atualizando o NMS em um agrupamento do MS Server

Em um agrupamento de tolerância a falhas do MS Server 2003/2008/2008 R2:

1. Atualize o NMS no nó principal (ativo), usando um dos procedimentos de atualização do Windows. Consulte:
   - Atualizando o NMS no Windows com a GUI do assistente de instalação (na página 17)
   - Atualizando o NMS no Windows, Linux ou Solaris com o modo silencioso (na página 19)
2. Torne ativo o nó secundário (passivo) e, em seguida, atualize o NMS usando o mesmo processo usado no nó principal.

Isso garante que as chaves de registro nos nós principal (ativo) e secundário (passivo) estão atualizados para a nova versão.

Atualizando os clientes do NMS

Atualização do Gerenciador de infraestrutura

Em todos os servidores e estações de trabalho que têm o Infrastructure Manager instalado (verifique em **Iniciar > Todos os Programas > Nimsoft Monitoring**), você deve fazer a atualização para a versão mais nova.

1. Abra um navegador web no computador em que deseja atualizar o Gerenciador de infraestrutura e acesse o Nimsoft Monitor Server na página da web no URL: <servername_or_server_IP_address>:8080.
2. Na página web exibida, escolha o link **Legacy Infrastructure Manager** para instalar a nova versão nesse computador.
3. Repita esse procedimento para atualizar outros computadores.

Observação: *o Console de administração do Nimsoft Monitor* fornece uma alternativa independente de plataforma para o Gerenciador de infraestrutura. Ele pode ser iniciado de forma autônoma em um navegador em <servername_or_server_IP_address>:8080 ou pode ser executado como um portlet no UMP.

Atualizar hubs

1. Identifique os sistemas que contêm um hub e uma infraestrutura secundária (consulte no Infrastructure Manager; confirme verificando em **Painel de Controle->Adicionar ou Remover Programas** no sistema cliente).

   Observação: a atualização de hubs secundários pode ser necessária somente se duas ou mais versões anteriores forem atualizadas. Consulte a seção Verificação da instalação ou atualização com êxito (na página 24) para versões do hub e de componentes incluídos nesta release, e compare aos hubs secundários instalados atualmente.

2. Salve uma cópia do arquivo hub.cfg na pasta Nimsoft\hub no sistema. Os parâmetros ideais de tempo limite para o hub atualizado são definidos durante a atualização, substituindo configurações de tempo limite existentes. A Nimsoft recomenda executar o hub atualizado com estes valores ideais para obter um desempenho aprimorado. No entanto, se deseja reverter para as configurações antigas de tempo limite por qualquer motivo, é importante manter um backup do antigo arquivo de configuração do hub.
3. No computador cliente, vá até a página do NMS na web (http://<servername_or_IP_address>:8080).
4. Na página web exibida, escolha o link **Robô do Windows, Hub, Servidor de distribuição,** para atualizar o hub e a infraestrutura do Nimsoft nesse computador.
5. Siga os prompts para concluir a instalação.
6. Repita esse procedimento para outras atualizações de hub.

Atualizar as filas do hub para a detecção

- Após uma atualização, certifique-se de que as informações da detecção de dispositivos (a partir de todos os probes distribuídos envolvidos na detecção automatizada) podem acessar o discovery_server. Isto requer:

  a. A criação de uma fila de anexos para o assunto do **probe_discovery** em todos os hubs secundários que hospedam o discovery_agent, o vmware ou o cm_data_import.

  b. A configuração de uma fila de obtenção com o assunto **probe_discovery** em cada hub, com exceção daqueles na parte inferior da hierarquia de hubs.

Consulte o *Guia do Usuário de Detecção* para obter todo o procedimento sobre como configurar as filas do probe_discovery.

Observação: se todos os componentes de detecção estiverem localizados sob o hub principal, essa comunicação será feita automaticamente, e nenhuma configuração manual de filas será necessária.

Atualização de robôs

Use um ou vários dos seguintes procedimentos para atualizar todos os robôs no seu domínio, incluindo os robôs nos hubs secundários.

Console de administração

1. Efetuar logon no Console de administração: http://<*nms_servername_or_IP*>:8080/adminconsole
2. Localize o pacote **robot_update** no **Arquivo**.
3. Arraste e solte o pacote no ícone do robô que deseja atualizar.

Infrastructure Manager

1. Inicie o Gerenciador de infraestrutura no hub primário atualizado (ou outro hub com um arquivo atualizado).
2. Localize o pacote **robot_update** no **Arquivo**.
3. Arraste e solte o pacote no ícone do robô que deseja atualizar.

Instalação manual

1. No sistema que contém o robô que deseja atualizar, navegue até a página da web do NMS (http://<*nms_servername_or_IP*>:8080).
2. Faça download do programa de instalação apropriado:
   - Windows: **robô do Windows**
   - UNIX/Linux: **utilitário de instalação UNIX/LINUX (nimldr) para todas as plataformas**
3. Inicie o programa de instalação e siga as etapas na tela para concluir a atualização.

Verificação de instalação ou atualização bem-sucedida

A Nimsoft recomenda verificar os resultados do processo de instalação a fim de detectar quaisquer falhas. Três indicativos de sucesso:

- É possível ver o **Nimsoft Server 7.6** na página web do NMS.
- Você tem as versões atuais de todos os componentes na janela principal do Infrastructure Manager e para as interfaces de usuário (selecione **Ajuda > Sobre** para verificar a versão).
- O novo probe mpse é exibido no Infrastructure Manager e no Console de administração.

Observação: estas tabelas listam os números de versão dos probes fornecidos com o NMS 7.6. Ocasionalmente, a Nimsoft fornece versões mais recentes de alguns probes entre as releases dos pacotes do servidor. As atualizações mais recentes de probes são exibidas no site de suporte da Nimsoft http://support.nimsoft.com http://support.nimsoft.com (nas páginas **Download** e **Arquivo morto**) à medida que ficam disponíveis.

Importante: a operação normal da execução do programa de instalação da Nimsoft, durante uma atualização, é substituir componentes e probes atualmente instalados. Em alguns casos, quando probes de "correção" ou versões especiais/atualizadas de componentes tiverem sido instalados anteriormente para solucionar problemas ou oferecer suporte a requisitos personalizados, a atualização poderá resultar em downgrades de componente. Se isso acontecer, as versões de probe e componentes necessários poderão ser restaurados localizando-os no NM Server Archive e instalando-os em vez do que foi fornecido pela atualização.

Interfaces do usuário	Versão 7.6	Release anterior
Infrastructure Manager	4.08	4.08
Console de administração	7.60	7.50
Dr. Nimbus	1.5.3	1.5.3
Componentes de back-end	**Versão 7.6**	**Release anterior**
alarm_enrichment	4.36	4.32
audit	1.22	1.22
automated_deployment_engine	1.31	1.30
baseline_engine	2.20	2.00
controller	7.60	7.05
data_engine	7.95	7.92
distsrv	5.30	5.30

fault_correlation_engine	1.66	1.66
hdb	7.60	7.05
hub	7.50	7.50
NAS	4.36	4.32
nimldr	3.57	3.57
nis_server	3.22	3.13
maintenance_mode	1.10	1.00
mpse	1.60	1.50
ppm	2.31	2.25
qos_processor	1.23	1.22
relationship_services	1.70	1.70
robot_update	7.60	7.05
service_host	7.60	7.50
sla_engine	3.62	3.62
spooler	7.60	7.05
Componentes da detecção	**Versão 7.6**	**Release anterior**
ace (versão de várias plataformas)	3.20	3.12
assetmgmt	1.24	1.24
cisco Monitor	3.36	3.36
cm_data_import	7.60	7.50
cdm	4.81	4.81
discovery_agent	7.60	7.50
discovery_server	7.60	7.50
interface_traffic	5.33	5.33
net_connect	3.02	3.02
rsp	4.00	4.00
topology_agent	1.69	1.69

Capítulo 5: Problemas conhecidos

As seções a seguir descrevem os problemas conhecidos e as soluções alternativas em alguns casos.

Desempenho, estabilidade e escalabilidade

ID do subsistema do mecanismo da linha de base

As IDs do subsistema nos alarmes de limite dinâmico geradas a partir do mecanismo de linha de base não correspondem às IDs de subsistema nos alarmes estáticos gerados dos probes.

Funcionalidade do robô

O robô 7.10 (o controlador, o spooler e os probes hdb) apresentaram problemas em alguns ambientes distintos. Se estiver usando com êxito a versão 7.10, poderá continuar a usá-la após a atualização para o NMS 7.6. Se estiver com problemas com a versão 7.10, recomendamos implantar o robô 7.05, que foi confirmado para trabalhar com o NMS 7.6.

Desempenho do hub em implantações de alto volume

Em implantações de alto volume, o hub 7.10 pode ter problemas quando usado como um hub de proxy LDAP ou quando usado com o probe SNMPCollector. Esses problemas foram corrigidos no hub 7.11 e 7.5.

Impacto potencial de filas inativas com encapsulamentos

Quando o hub 7.10 usa um servidor de encapsulamento, o número de recursos usados para os identificadores de arquivo do Windows e os descritores de arquivo Unix pode crescer de forma estável ao longo do tempo. A taxa de crescimento aumenta consideravelmente quando o servidor de encapsulamentos está atendendo a uma ou mais filas *get* que contêm pouco ou nenhum dado e, por isso, redefinidas regularmente. À medida que o número de recursos em uso cresce, o hub pode reiniciar automaticamente e retornar à operação normal. Não se espera nenhuma perda de dados durante esses reinícios e o sistema deve voltar automaticamente à operação normal.

As versões 7.11 e 7.5 do hub resolvem esses problemas.

ADE (Automated Deployment Engine - Mecanismo de Implantação Automatizada)

A distribuição do robô ADE para destinos do Windows às vezes falha ao ativar os probes hdb e spooler.

Para resolver esse problema, vá para a máquina afetada e execute uma **validação de segurança** nos probes afetados (hdb e spooler).

Reinicialização lenta do discovery_server no MySQL

Quando o Servidor de detecção é iniciado, ele executa um script para verificar/criar tabelas no banco de dados do NIS. Na versão 5.5 do MySQL existe um erro (consulte http://bugs.mysql.com/bug.php?id=63144 e http://dev.mysql.com/doc/relnotes/mysql/5.6/en/news-5-6-13.html) que faz com que a execução desse script seja lenta.

A atualização do MySQL para a versão 5.6.13 ou posterior resolve esse problema.

Ao usar o fluxo 5.5 do MySQL, a solução de contorno é desativar dashboard_engine e encerrar quaisquer consultas pendentes durante a reinicialização do servidor de detecção. Isso possibilitará que o script de criação de detecção prossiga.

Red Hat Enterprise Linux (RHEL)

Os processos do Nimsoft no RHEL 6.1 x86-64 consumem mais memória do que em outras plataformas Linux.

- **Sistemas RHEL v6 de 64 bits**

  Os processos podem utilizar até três vezes a quantidade de memória virtual e residente por processo, em comparação às releases anteriores do RHEL ou a outros sistemas operacionais.

- **Sistemas RHEL v6 de 32 bits**

  Os processos podem utilizar várias vezes mais memória virtual, mas a memória residente por processo é basicamente equivalente.

Facilidade

- **O erro nametoip pode ser exibido**

  Ao atualizar para o NMS 6.0, você pode ver **nametoip** listado como um erro fatal no **ace.log** e no **nis_server.log**. Ele pode ser ignorado. O controlador observa que o ACE encontrou esse erro e reinicia automaticamente o ACE, o que corrige o erro.

- **Ocorrências de permissão no Windows 2008**

  Privilégios de gravação são necessários para gravar na pasta Arquivos de programas do Nimsoft. Se você efetuar logon como um usuário sem privilégios de administrador, após a instalação, você deverá definir manualmente esses privilégios de gravação.

- **A comunicação com o robô pela rede falha devido ao arquivo /etc/hosts inválido**

  Apenas sistemas que não sejam o Windows

  Certifique-se de que o arquivo **/etc/hosts** em qualquer sistema que não seja o Windows hospedando um robô, hub, servidor ou instância UMP do Nimsoft contém uma entrada válida para o computador local. Esse deve ser um par totalmente qualificado de nome do host e endereço IP. Se apenas loopback for definido (por exemplo, localhost 127.0.0.1), o probe do controlador nesse computador não terá conhecimento do seu próprio endereço IP, resultando em uma falha na comunicação de rede.

- **Ativando a detecção e a configuração de um probe interface_traffic existente no servidor**

  A função de detecção do Nimsoft ativa automaticamente a criptografia de sequências de caracteres da comunidade no arquivo de configuração do probe no computador da detecção. Antes de ativar a função de detecção, ative a criptografia no probe de tráfego da interface. Caso isso não seja feito, as configurações existentes param de funcionar devido às sequências de caracteres da comunidade inválidas. Os probes Interface_traffic em outros robôs não são afetados.

- **A instalação silenciosa requer um valor DB_PORT se você usar portas dinâmicas**

  Se estiver instalando com as instâncias nomeadas do MS SQL Server ou com o SQL Server Express e estiver usando portas dinâmicas, você não poderá usar o número de porta padrão (1433), pois isso impedirá que data_engine se conecte ao banco de dados.

  Data_engine ficará verde no Infrastructure Manager (porque está em execução), mas a falta de conexão fará com que a fila aumente continuamente.

  Se a porta padrão tiver sido usada:

  1. No Infrastructure Manager, abra a GUI de configuração do probe data_engine, clicando duas vezes no objeto data_engine.
  2. Na guia Banco de dados, exclua a vírgula e o número da porta (**,1433**) anexados ao nome do servidor do banco de dados.
  3. Especifique a porta correta e, em seguida, reinicie o probe.

- **Correlação de falhas é afetado pela configuração de encaminhamento de alarmes do hub e pela replicação de alarme do NAS**

  Para que o aplicativo Correlação de falhas forneça resultados precisos, certifique-se de que os alarmes e as mensagens de interface_poller dos hubs nas áreas aplicáveis da sua topologia de rede estão sendo encaminhados para o hub em que o FCE (Fault Correlation Engine - Mecanismo de Correlação de Falhas) está em execução. Você deve usar as filas do hub que incluem os assuntos **alarme** e **interface_poller** para encaminhar as mensagens que o FCE exige. Use as filas POST ou GET se desejar enviar ou receber mensagens de um hub para o outro.

  Importante: não ative a replicação de alarme do NAS ou o encaminhamento de alarmes ao usar o FCE, pois isso fará com que os alarmes sejam processados duas vezes e gerará resultados imprevisíveis.

- **Os usuários do MySQL devem desativar o probe qos_processor antes da instalação/atualização do UMP**

  Quando o UMP estiver instalado, o processador de QoS poderá ser reativado.

- **Alguns probes talvez não sejam iniciados após a instalação**

  Alguns probes podem não ser iniciados após a instalação do NMS, devido à ausência de recursos do sistema disponíveis.

  Para corrigir esse problema, edite a chave de registro HKEY_LOCAL_MACHINE\System \CurrentControlSet \Control \Session Manager\SubSystems\Windows:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,3072,512,Windows=On SubSystemType=Windows
ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off
MaxRequestThreads=16
```

  Altere o valor 512 (em texto em **negrito** no exemplo acima) para **1024**.

  Para obter mais informações, consulte o artigo em http://support.microsoft.com/kb/184802 http://support.microsoft.com/kb/184802.

- **Os probes do UMP precisam ser reinicializados após a atualização para o NMS 6.0**

  Se você tiver o UMP instalado, reinicie os probes **wasp** e **dashboard_engine** para evitar quaisquer ocorrências durante o logon no UMP após a atualização do NMS.

- **Os probes não são ativados após a instalação do servidor do Nimsoft**

  Vários componentes são distribuídos e configurados durante a instalação do NMS. Em sistemas mais lentos, alguns probes podem não ser iniciados após a instalação. Isso pode ser detectado no Infrastructure Manager e geralmente é corrigido por meio da ativação manual do probe.

- **Os usuários do Oracle precisam adicionar uma chave ao probe dashboard_engine**

  Durante a instalação do NMS, o programa de instalação tenta configurar a conexão com o banco de dado Oracle.

  Observação: quando for solicitado que você digite um nome de serviço, digite primeiro o SID para o espaço de tabela que planeja usar. Se o sistema informar que não pode se conectar ao banco de dados usando o SID, digite um nome de serviço.

  Se você tiver usado um nome de serviço em vez de um SID, ao final da instalação do UMP você poderá ver uma mensagem de erro listando os probes (que exigem conexão com o banco de dados) cuja inicialização falhou. Se isso ocorrer, adicione uma **Chave** e um **Valor** ao probe dashboard_engine. Isso irá reparar a conexão com o banco de dados do dashboard_engine e permitir a inicialização de quaisquer probes que dependam dela.

Siga estas etapas:

1. Abra o Infrastructure Manager e localize o probe dashboard_engine sob o nó **Serviço**.
2. No dashboard_engine, clique Shift + botão direito do mouse na lista de probes à direita para abrir a caixa de diálogo **Raw Configure**.
3. Abra a pasta **Dados** e adicione a **Chave** e o **Valor** a seguir.

   Chave: jdbc_url_template

   Valor: jdbc:oracle:thin:{1}/{2}@{0}:{7}:{your_SID}
4. Aplique a nova chave e valor e reinicie o dashboard_engine.

- **Computadores com AIX não são encontrados pela detecção usando SNMP**

  Ao usar SNMP, determinados tipos de computadores com AIX podem não ser encontrados porque o formato no campo de descrição do computador não pode ser lido. (O AIX envia dados binários como descrição pela API de SNMP que o NMS usa.)

- **Problemas no banco de dados SQLite no Solaris 9**

  Você pode ver os erros SQLITE_BUSY ou SQLITE_CORRUPT no discovery_agent.log. Esses erros podem ser ignorados, contanto que sejam esporádicos e o **discovery_agent** pareça funcionar (por exemplo, continua a detectar novos sistemas e atualiza o "tempo de atividade" dos sistemas monitorados).

  Uma ocorrência mais séria é quando o discovery_agent para de funcionar e você vê o seguinte erro durante a inicialização:

```
Failed to initialize the database file, correct the error and start the probe again.
```

  Para corrigir o problema:

  1. Desative o discovery_agent.
  2. Exclua os arquivos **.db3** e **.dbz** do diretório do discovery_agent:

     <Nimsoft_install_folder>\probes\service\discovery_agent*.db3

     <Nimsoft_install_folder>\probes\service\discovery_agent*.dbz
  3. Ative o discovery_agent.

- **O agente de detecção não funciona em um robô passivo**

  A Nimsoft está investigando uma possível correção em uma futura release.

Implantação de robôs em AIX e zLinux

Não é possível usar o USM (Unified Service Manager – Gerenciador de Serviços Unificados) para implantar automaticamente robôs em sistemas AIX ou zLinux que foram colocados em seu inventário por meio da detecção automatizada. Para implantar robôs nesses sistemas, faça o seguinte:

- Use o probe do ADE (Automated Deployment Engine) com um arquivo XML. Consulte Implantação em massa com o probe ADE no Guia de Instalação do NMS.
- Use os programas de instalação nativos. Consulte Instalação de robôs e hubs secundários em Linux ou Solaris no Guia de Instalação do NMS.
- Importe um arquivo XML no USM. Consulte Implantar robôs em sistemas listados em um arquivo na ajuda do Gerenciador de serviços unificados do UMP.

GUI do Console de administração v7.92 do data_engine

Os seguintes campos na GUI do Console de administração v7.92 do data_engine não estão funcionais:

- Nó **data_engine**:
  - Campo **Excluir dados históricos mais antigos que**
- Nó **Qualidade de serviço**:
  - Seleção **Substituir tempo de vida médio diário**
  - Campo **Tempo de vida médio diário**

Esses campos serão ativados em uma release futura.

Autenticação de senha de detecção

O agente de detecção usa a autenticação de senha para se conectar a um dispositivo de destino por meio de SSH. O agente de detecção não pode se comunicar com um dispositivo em que o SSH está configurado para outros métodos de autenticação, como interativo por teclado. O Agente de detecção também não oferece suporte à autenticação de chave pública nem à autenticação desafio-resposta.

Console de administração: não foi possível aceitar o certificado SSL no UMP

Problema:

Esse problema ocorre quando Console de administração está configurado para usar um certificado SSL autoassinado para a comunicação com o processo do service_host no NMS.

Ao iniciar o Console de administração como um portlet no UMP pela primeira vez, você receberá um erro 501 informando que o certificado SSL autoassinado não é confiável, mas não será fornecido nenhum meio para aceitar o certificado e continuar. Isso ocorre devido a uma limitação de como alguns navegadores lidam com os certificados SSL dentro de um iframe seguro.

Solução:

Para solucionar esse problema, abra primeiro o Console de administração autônomo em um navegador da web (https://<NMS_host>:8443), onde você poderá ver a mesma mensagem de segurança e poderá aceitar o certificado. Em seguida, o Console de administração será aberto no UMP (no mesmo navegador, no mesmo endereço IP) sem esse problema.

Como alternativa, na caixa de diálogo de erro no UMP que o navegador mostra (o certificado não é confiável. Não foi possível estabelecer a comunicação com o <URL>), copie o URL específico e cole em outra janela ou guia do navegador (no mesmo navegador que está executando o UMP) e aceite o certificado. Retorne ao UMP e recarregue a página para limpar o erro 50.

O link do Gerenciador de NiS no Infrastructure Manager não funciona

Sintoma

Quando eu clico no link do Gerenciador de NiS no Infrastructure Manager, recebo uma mensagem de erro: "Erro ao executar o comando: C:\Arquivos de Programas (x86)\Nimsoft\bin\NiSmgr.exe."

Causa

O aplicativo do Gerenciador de NIS foi removido da versão mais recente do NMS. Para configurar componentes de detecção, visite o Assistente de detecção localizado no Portlet do USM.

ADE: use a autenticação de senha de SSH wtih OpenSUSE12.x

Por padrão, o OpenSUSE desativa a autenticação de senha do SSH. Se desejar usar a autenticação de senha de SSH, siga estas etapas:

1. Abra o arquivo /etc/sshd_config com um editor.
2. Localize a entrada "PasswordAuthentication no" e altere para "PasswordAuthentication yes"
3. Salve o arquivo e feche o editor.

Se você não usar a autenticação de senha, você deve usar a autenticação de chave pública de RSA. Consulte a seção Valores de parâmetro para host-profiles.xml no Apêndice A: Implantação em massa com mecanismo de implantação automatizada no Guia de Instalação do NMS. A documentação está disponível na biblioteca de documentação do Nimsoft.

O probe PPM não é suportado no AIX

O probe PPM não será executado em hubs do AIX. Para configurar robôs e probes em hubs do AIX, use a configuração simples com base na web ou o Gerenciador de infraestrutura herdado.

Ocorrências de permissão no Windows 2008

Privilégios de gravação são necessários para gravar na pasta Arquivos de programas do Nimsoft. Se você efetuar logon como um usuário sem privilégios de administrador, após a instalação, você deverá definir manualmente esses privilégios de gravação.

Encaminhamento de alarme do hub e replicação de alarme do NAS afeta a correlação de falha

Problema:

A correlação de falhas é afetada pela configuração de encaminhamento de alarmes do hub e pela replicação de alarme do NAS.

Solução:

Para que o aplicativo Correlação de falhas forneça resultados precisos, certifique-se de que os alarmes e as mensagens de interface_poller dos hubs nas áreas aplicáveis da sua topologia de rede estão sendo encaminhados para o hub onde o probe FCE (Fault Correlation Engine - Mecanismo de Correlação de Falhas) está em execução. Você deve usar as filas do hub que incluem os assuntos alarme e interface_poller para encaminhar as mensagens que o FCE exige. Use as filas POST ou GET se desejar enviar ou receber mensagens de um hub para o outro.

Importante: não permita a replicação de alarme do NAS ou encaminhamento ao usar FCE. Isso faz com que os alarmes sejam processados duas vezes e produz resultados imprevisíveis.

UNIX: a comunicação do robô falha devido /etc/hosts inválidos

Problema:

Em sistemas que não são Windows, a comunicação do robô pela rede falha devido ao arquivo /etc/hosts inválido.

Solução:

Certifique-se de que o arquivo **/etc/hosts** em qualquer sistema que não seja o Windows hospedando um robô, hub, servidor ou instância UMP contendo uma entrada válida para o computador local. Esse deve ser um par totalmente qualificado de nome do host e endereço IP. Se apenas loopback for definido (por exemplo, localhost 127.0.0.1), o probe do controlador nesse computador não terá conhecimento do seu próprio endereço IP, resultando em uma falha na comunicação de rede.

Não foi possível encontrar um dispositivo no USM pelo endereço IP

Como parte dos aprimoramentos do servidor de detecção e do agente de detecção 7.0, um dispositivo com vários endereços IP agora é exibido como um único dispositivo no USM (Unified Service Manager - Gerenciador de Serviços Unificados) e não como vários dispositivos distintos por endereço IP. Se não for possível localizar um dispositivo no USM por um endereço IP, tente pesquisar pelo nome.

Localização

Sequências de caracteres traduzidas são erros no arquivo de log de instalação (iaoutput.txt).

Instalação

Falha na instalação devido à versão do Java JRE

O programa de instalação de pré-verificação pode indicar um problema com o Java Runtime Environment (JRE) se ele encontrar a versão 29 ou 30 do Java 6 (JRE 1.6.29 ou 1.6.30).

Observação: há um problema conhecido com o JRE 1.6.29 e o 1.6.30 (Java 6 versões 29 e 30) ao trabalhar com o MS SQL Server (consulte: http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7105007) http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=7105007.

A Nimsoft recomenda que você instale a atualização mais recente do JRE SE 6 ou SE 7, dependendo de qual versão você esteja usando. Para o JRE 6, ele é atualmente o JRE 1.6u43 (Java 6 atualização 43). Para JRE 7, ele é 1.7u17 (Java 7 atualização 17).

Observação: a instalação no Windows Server 2012 exige o JRE 1.6u38 / 1.7u6 ou posterior para que a plataforma do sistema operacional seja detectada de forma adequada.

Solaris apenas:

A pré-validação do programa de instalação sinaliza quando um JRE de 32 bits é instalado em uma plataforma Solaris de 64 bits. Com o Solaris, o uso do JRE de 64 bits como referência JRE para o NMS é obrigatório.

- Certifique-se de que possui um JRE de 64 bits instalado antes de executar o programa de instalação.
- Além disso, verifique o PATH para ver se (1) um JRE de 64 bits está listado e (2) listado antes de qualquer JRE de 32 bits.

Observação: o Solaris é diferente de outras plataformas uma vez que o JRE de 64 bits está localizado um diretório mais abaixo.

Em sistemas AMD64, o caminho completo para o diretório JRE de 64 bits é normalmente:

```
/usr/java/jre/bin/amd64
```

Em sistemas SPARC, o caminho completo para o diretório JRE de 64 bits é normalmente:

```
/usr/java/jre/bin/sparcv9
```

- Verifique se o PATH inclui o diretório JRE de 64 bits e, em seguida, execute novamente o programa de instalação.

O agente de detecção e outros probes emitem alarme de ocorrência na atualização

Sintoma

O agente de detecção e alguns outros probes podem enviar um único alarme informativo ao atualizar para a versão mais recente do NMS. Esse alarme é benigno e pode ser ignorado com segurança.

Causa

O Servidor de detecção cria uma fila de barramentos dos quais esses outros probes dependem. A fila pode não estar totalmente operacional quando esses probes são ativados, o que faz com que o alarme informativo seja enviado. A fila será ativada em um curto período de tempo.

A instalação do NMS falha no CentOS, OpenSuse e RHEL

Sintoma

A instalação do servidor do NM falha no CentOS, no OpenSUSE versão 12 ou no RHEL de 32 bits.

Causa

O Mecanismo de dados requer libstdc++.so.5 { libstdc++-3.3.4-11.x86_64.rpm }

A instalação do lib compatível resolve o problema.

Emita este comando:

```
yum install compat-libstdc++-33
```

Recomendável: implantar o PPM para cada hub no seu domínio

Para usar a configuração com base na web para qualquer hub remoto ou robôs/probes nesse hub, o PPM precisa ser distribuído para esse hub.A Nimsoft recomenda que o PPM seja implantado em cada hub dentro de seu domínio.

Alguns probes talvez não sejam iniciados após a instalação

- **Instalação do NMS no Windows**

  Após instalação do NMS em sistemas Windows, alguns probes podem não iniciar devido à falta de recursos disponíveis do sistema.

  Para corrigir esse problema, edite a chave de registro HKEY_LOCAL_MACHINE\System \CurrentControlSet \Control \Session Manager\SubSystems\Windows:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512,Windows=On
SubSystemType=Windows ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16
```

  Altere o valor 512 (em texto em **negrito** no exemplo acima) para **1024**.

  Para obter mais informações, consulte o artigo em http://support.microsoft.com/kb/184802.

- **Instalação do NMS em todas as plataformas**

  Vários componentes são distribuídos e configurados durante a instalação do NMS. Em sistemas mais lentos, alguns probes podem não ser iniciados após a instalação. Isso pode ser detectado no Gerenciador de infraestrutura ou no Console de administração e é corrigido por meio da ativação manual do probe.

- Atualização do **NMS em todas as plataformas**

  Se você atualizar para o NMS e possui o UMP instalado, reinicie os probes **wasp** e **dashboard_engine** para evitar qualquer problema ao efetuar o logon no UMP após a atualização.

Instalação do UMP no MySQL

Os usuários do MySQL devem desativar o probe QoS_processor antes de instalar ou atualizar o UMP no NMS 6.50. Quando o UMP estiver instalado, o processador de QoS poderá ser reativado.

ADE: Instalando o robô em Debian v6

Por padrão, o Debian v6 usa o endereço 127.0.1.1 como o endereço de resolução de nomes. Quando um robô é implantado em um sistema Debian 6 usando ADE, após a reinicialização do sistema o robô tentará vincular-se a 127.0.1.1, pois é o endereço disponível. Use a seguinte solução alternativa para evitar a contenção de 127.0.1.1 no sistema Debian 6:

1. Ao instalar o robô *manualmente* ou com o *ADE*, é necessário ir até o sistema de destino após a operação e adicionar a linha a seguir ao arquivo robot.cfg:

   ```
   robotip = ip_address
   ```

   em que **ip_address** é o endereço IP a que o robô deve se vincular no computador de destino.

2. Ao implantar uma caixa de Debian 6.0.5 usando *XML*, é necessário definir a opção **<robotip>ip_address</robotip>**, em que **ip_address** é o endereço a que o robô deve se vincular no computador de destino.

Autenticação LDAP: usuários do grupo do administrador que não seja do domínio não podem efetuar logon no servidor do NM

Um usuário LDAP não poderá efetuar logon no servidor do NMS exceto se o usuário do Active Directory for um integrante do grupo do administrador do domínio LDAP. A diretiva de grupo do LDAP no NMS não importa.

A instalação silenciosa com o SQL Server e portas dinâmicas requer DB-PORT

Se estiver instalando com as instâncias nomeadas do MS SQL Server ou com o SQL Server Express e estiver usando portas dinâmicas, você não poderá usar o número de porta padrão (1433), pois isso impedirá que data_engine se conecte ao banco de dados.

Data_engine ficará verde no Infrastructure Manager (porque está em execução), mas a falta de conexão fará com que a fila aumente continuamente.

Se a porta padrão tiver sido usada:

1. No Infrastructure Manager, abra a GUI de configuração do probe data_engine, clicando duas vezes no objeto data_engine.
2. Na guia **Banco de dados**, exclua a vírgula e o número da porta (**,1433**) anexados ao nome do servidor do banco de dados.
3. Especifique a porta correta e, em seguida, reinicie o probe.

Solaris: Falha na instalação reduz o espaço de troca disponível

Se a instalação do NMS for interrompida ou falhar por qualquer razão, os arquivos de instalação (/tmp/install.*) não são excluídos. Como a troca no Solaris inclui o diretório /tmp, a Nimsoft recomenda excluir manualmente esses arquivos antes de executar o programa de instalação novamente.

Linux com o MySQL: o acesso foi negado para o usuário root

Problema:

Ao tentar instalar o NMS com um banco de dados MySQL, você poderá ver o erro a seguir (ou seu equivalente) depois de digitar as informações do servidor de banco de dados:

```
ERROR 1045 (28000): Access denied for user 'root'@'<your Nimsoft hostname>' (using password: YES)
```

Isto ocorre porque os privilégios remotos não foram estabelecidos ou porque a senha identificada para os sistemas remotos não está de acordo com aquela definida no servidor de banco de dados localmente.

Solução:

Execute estas etapas:

1. Efetue logon no banco de dados MySQL localmente (ou seja, no servidor que hospeda o MySQL).
2. Para configurar o acesso de qualquer host, execute:

```
mysql> use mysql;
mysql> UPDATE user SET password=PASSWORD("<your password>") where User = 'root';
mysql> GRANT ALL PRIVILEGES ON *.* TO root@'%' IDENTIFIED BY '<your password>' WITH GRANT OPTION;
mysql> GRANT TRIGGER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql> GRANT SUPER ON *.* TO root@'%' IDENTIFIED BY '<your password>';
mysql> FLUSH PRIVILEGES
```

Para definir o acesso de um determinado host, execute estes comandos, substituindo *HostX* pelo nome do seu host:

```
mysql> use mysql;
mysql> UPDATE user SET password=PASSWORD("<your password>") where User = 'root' AND Host = 'HostX';
mysql> GRANT ALL PRIVILEGES ON *.* TO root@'HostX' IDENTIFIED BY '<your password>' WITH GRANT OPTION;
mysql> GRANT TRIGGER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql> GRANT SUPER ON *.* TO root@'HostX' IDENTIFIED BY '<your password>';
mysql> FLUSH PRIVILEGES;
```

Erro de IP inválido ao instalar a infraestrutura do Windows

Problema:

Quando executa o **NimBUS Infrastructure.exe** para instalar o robô do Windows, o hub e o servidor de distribuição, poderá ver a seguinte mensagem de erro:

```
IP da linha de comando não é válido: 127.0.0.1
```

Solução:

Esse erro é inofensivo e pode ser ignorado com segurança. Clique em OK e continue.

Capítulo 6: Defeitos corrigidos no NMS 7.6

Hub e robô

- Uma mensagem de erro falsa era por vezes apresentada quando um hub era expandido na árvore de navegação do Console de administração.
- As transferências em massa do robô para o hub falhavam ocasionalmente.

Detecção

- Em algumas configurações de rede em sistemas Unix (especialmente Solaris), o agente de detecção encontrava um erro esperando certas informações. Isso fez com que o agente de detecção terminasse antes de todos os resultados serem publicados. Agora o agente irá coletar as informações da melhor forma que puder e continuará detectando e publicando.
- O servidor de detecção inclui uma nova versão do SDK para fornecer um melhor desempenho em sistemas com várias interfaces de rede sendo executadas em diferentes sub-redes.
- Quando um robô executando um agente de detecção era movido de um hub para outro, era criado um registro extra do agente de detecção. Agora, o mesmo registro do agente de detecção (incluindo a configuração de detecção do agente) é mantido após o robô ser movido para outro hub.